US011227266B2

(12) **United States Patent**
Moiyallah, Jr. et al.

(10) **Patent No.: US 11,227,266 B2**
(45) **Date of Patent: Jan. 18, 2022**

(54) **DIGITAL HOLDING ACCOUNT**

(71) Applicant: **Bank of America Corporation**, Charlotte, NC (US)

(72) Inventors: **Samuel M. Moiyallah, Jr.**, Newark, DE (US); **Joseph Castinado**, Northglenn, CO (US)

(73) Assignee: **Bank of America Corporation**, Charlotte, NC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/699,692**

(22) Filed: **Dec. 1, 2019**

(65) **Prior Publication Data**

US 2021/0166206 A1 Jun. 3, 2021

(51) **Int. Cl.**

G06Q 40/08	(2012.01)
G06Q 20/10	(2012.01)
G06Q 20/40	(2012.01)
G06Q 20/36	(2012.01)
G06Q 20/38	(2012.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/10*** (2013.01); ***G06Q 20/363*** (2013.01); ***G06Q 20/367*** (2013.01); ***G06Q 20/382*** (2013.01); ***G06Q 20/385*** (2013.01); ***G06Q 20/40*** (2013.01); *G06Q 2220/00* (2013.01)

(58) **Field of Classification Search**

USPC 75/39; 705/39

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,600,009	B1 *	3/2020	Augustine	G06F 16/1837
2011/0258686	A1 *	10/2011	Raj	G06Q 20/10 726/6
2018/0268382	A1 *	9/2018	Wasserman	G06Q 20/0655
2018/0330342	A1 *	11/2018	Prakash	G06Q 20/4014

(Continued)

OTHER PUBLICATIONS

Augmenting Fiat Currency with an Integrated Managed Cryptocurrency; Publication date: Dec. 2019; Authors: Mell, Peter; http://arxiv.org/licenses/nonexclusive-distrib/1.0/ (Year: 2019).*

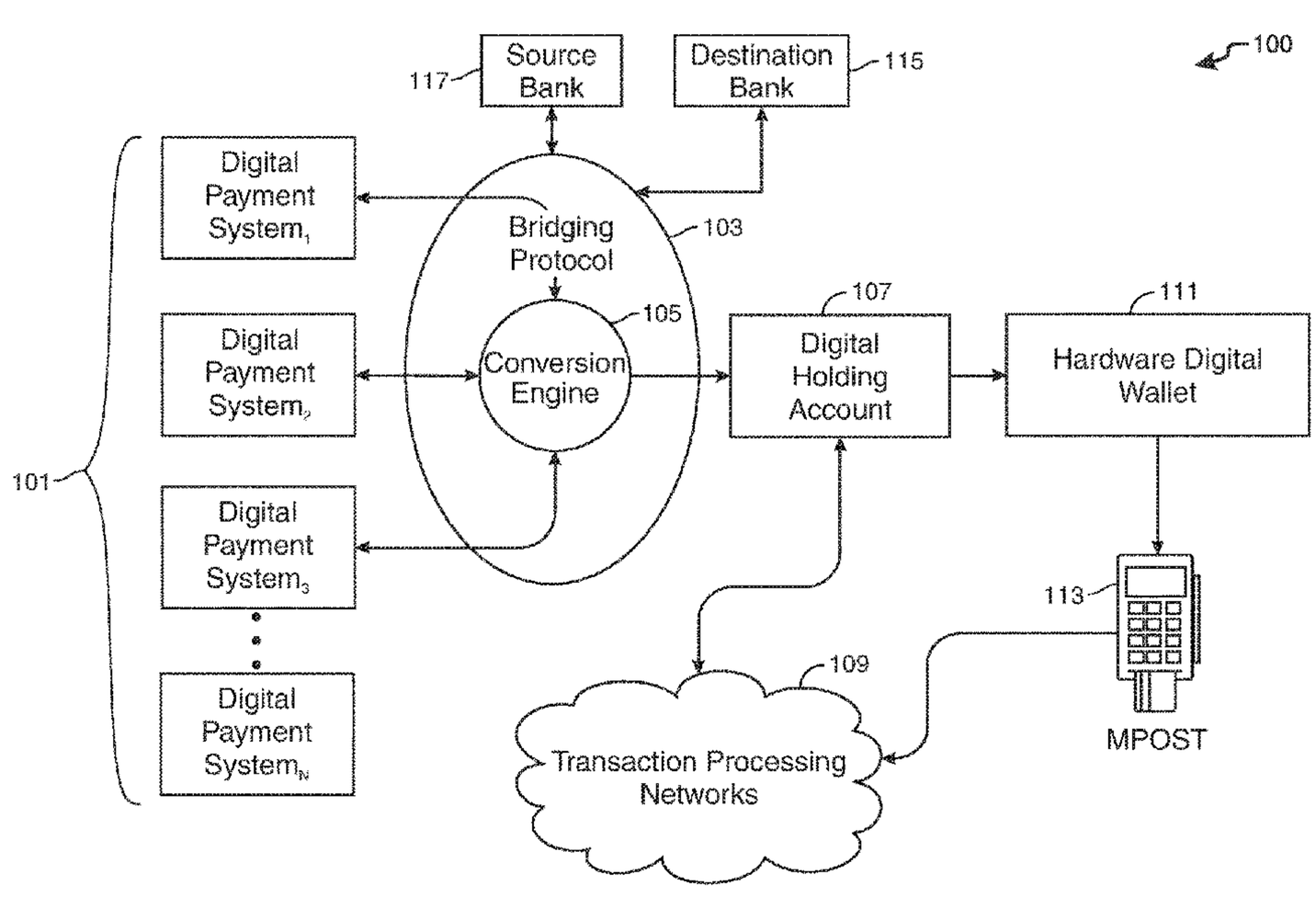
(Continued)

Primary Examiner — Hani M Kazimi
Assistant Examiner — Hatem M Ali
(74) *Attorney, Agent, or Firm* — Weiss & Arons LLP; Michael A. Springs, Esq.

(57) **ABSTRACT**

As the world progresses towards a cashless payment society, there has been a rise in the various forms of emerging payment technologies. Such technologies may include digital wallet payment systems. There is a need for a bridging protocol and conversion engine that would connect gaps between these various emerging payment technologies and their respective proprietary ecosystems. There is also a need for a digital holding account that provides a protective layer to fund transfers between cashless ecosystems. The digital holding account may hold and monitor currency processed by the conversion engine. Such currency would not be transferred directly into checking account. The digital holding account may be subject to rigorous validations to scrutinize the source and destination of transferred currency. Validation may include checking distributed ledger transaction records of prior transfers of the received currency.

16 Claims, 9 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2019/0180558	A1*	6/2019	Merati	G06Q 20/3678
2020/0302745	A1*	9/2020	Merati	G07F 17/3244

OTHER PUBLICATIONS

Distributed Ledger Privacy: Ring Signatures, M\"obius and CryptoNote; Publication Date: Feb. 7, 2019; Authors: Clack, Christopher D. • Courtois, Nicolas T. http://creativecommons.org/licenses/by/4.0/ (Year: 2019).*

Analysis of Blockchain System With Token-Based Bookkeeping Method; Publication Date: Jan. 1, 2019; Authors: Tianqi Cai • H. J. Cai • Hao Wang • Xiji Cheng • Linfeng Wang [+details]; EEE Xplore | IEEE Periodicals | Jan. 1, 2019 | IEEE Access (Year: 2019).*

Miller et al., "Detection Theory for Graphs," https://www.ll.mit.edu/r-d/publications/detection-theory-graphs, Lincoln Laboratory Journal, vol. 20, Jan. 30, 2013.

"Finding Patterns in an Unknown Graph," https://www.deepdyve.com/lp/ios-press/finding-patterns-in-an-unknown-graph-bxF0rxCnV1, A1 Communications, Jan. 2012.

Noble et al., "Graph-Based Anomaly Detection," http://www.ailab.wsu.edu/subdue/papers/NobleKDD03.pdf, ACM, Aug. 2003.

* cited by examiner

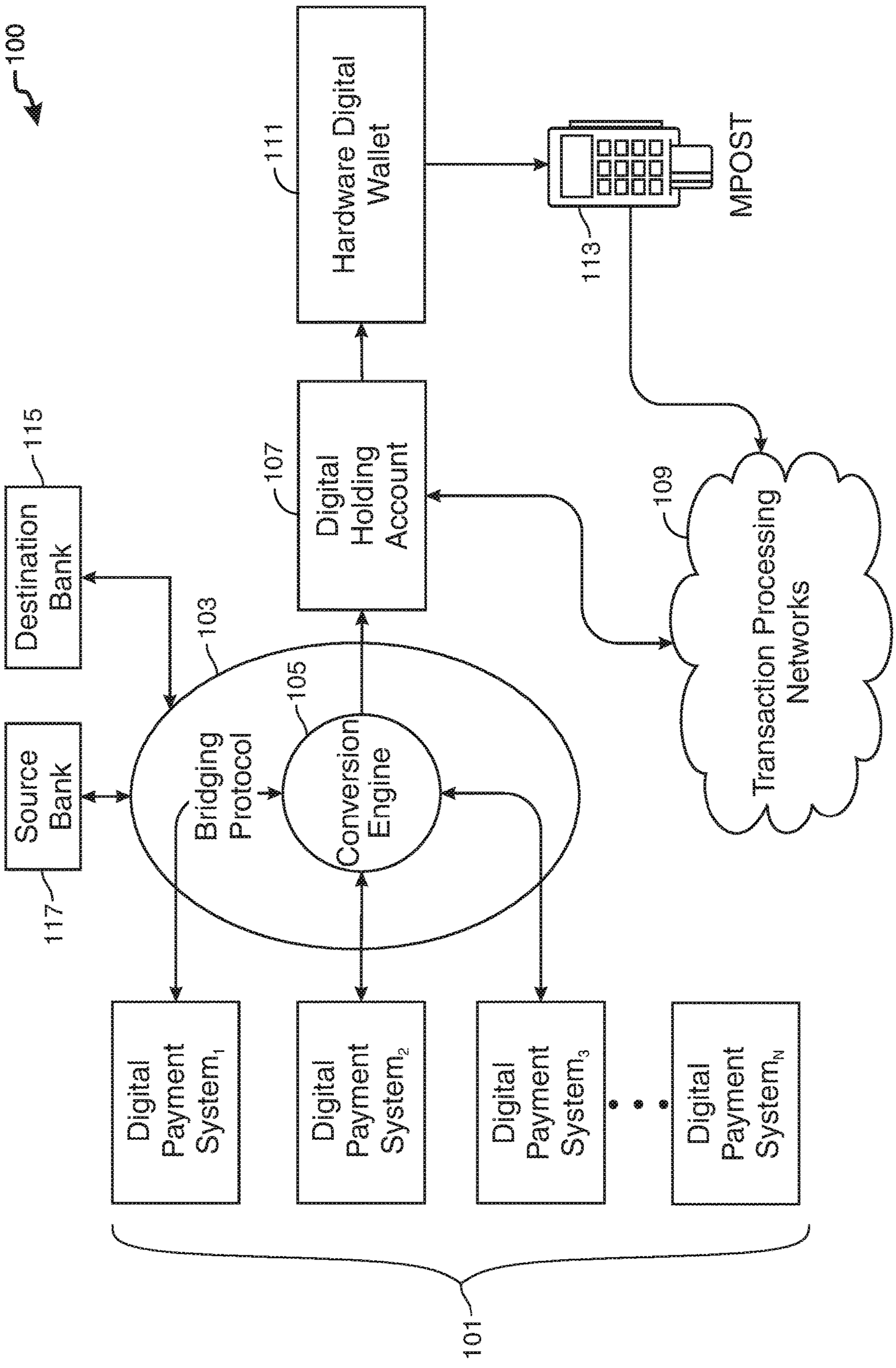

100
111
Hardware Digital Wallet
113
MPOST
115
Destination Bank
107
Digital Holding Account
109
Transaction Processing Networks
103
Source Bank
Bridging Protocol
105
Conversion Engine
117
Digital Payment System1
Digital Payment System2
Digital Payment System3
Digital Payment SystemN
101

FIG. 1

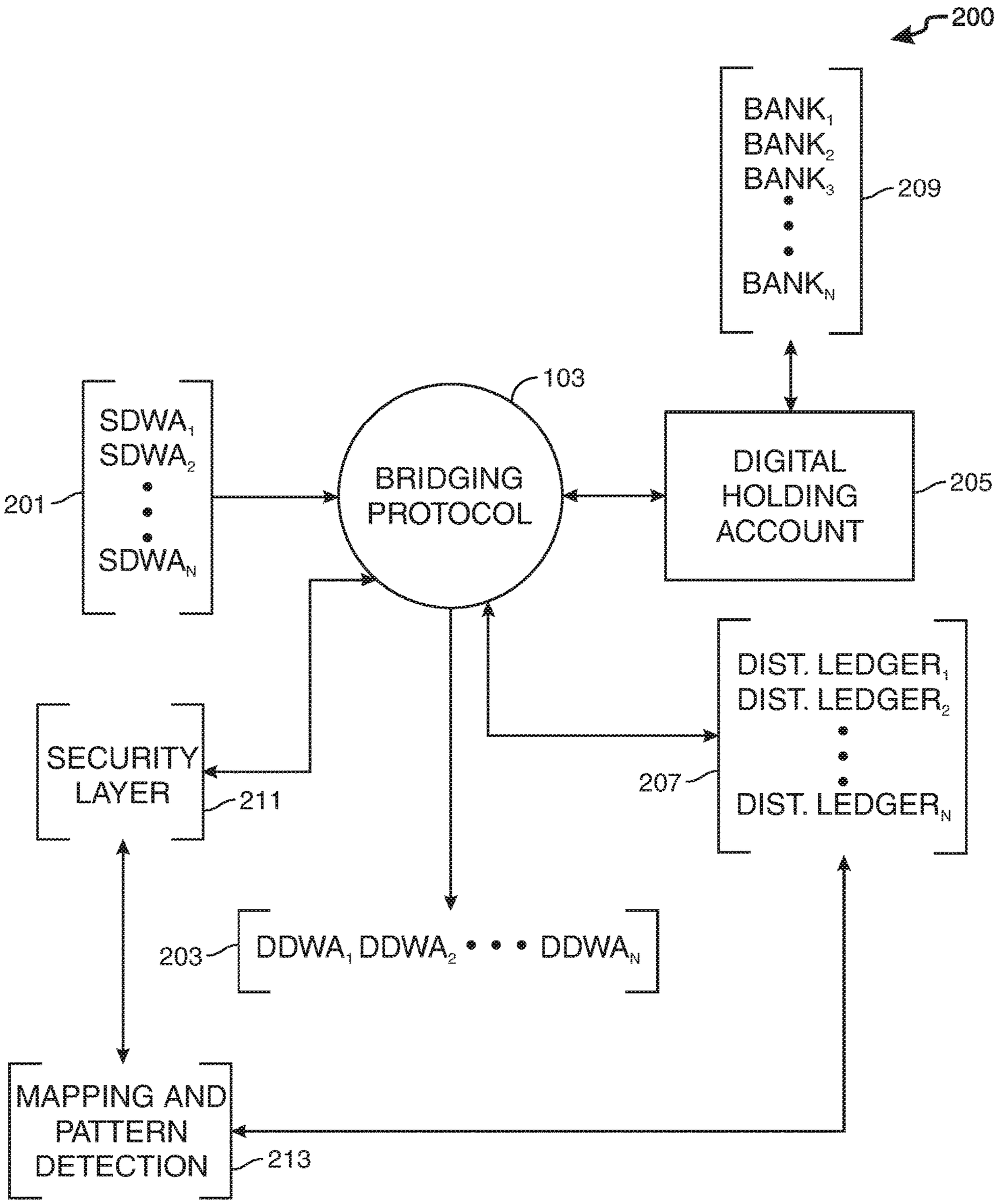

200
BANK1
BANK2
BANK3
BANKN
209
SDWA1
SDWA2
SDWAN
201
103
BRIDGING PROTOCOL
DIGITAL HOLDING ACCOUNT
205
SECURITY LAYER
211
DIST. LEDGER1
DIST. LEDGER2
DIST. LEDGERN
207
DDWA1 DDWA2 • • • DDWAN
203
MAPPING AND PATTERN DETECTION
213

FIG. 2

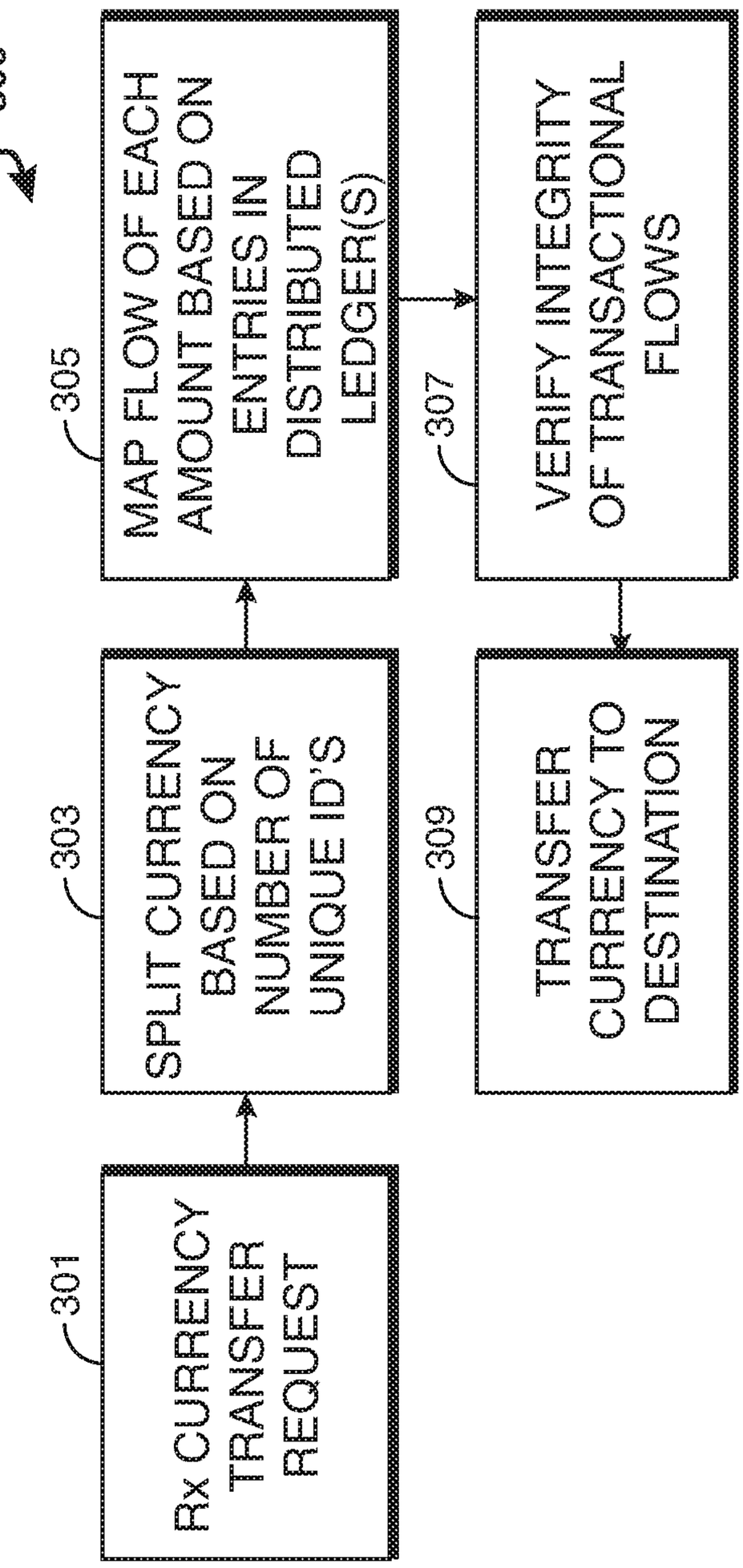

300
Rx CURRENCY TRANSFER REQUEST
301
SPLIT CURRENCY BASED ON NUMBER OF UNIQUE ID'S
303
MAP FLOW OF EACH AMOUNT BASED ON ENTRIES IN DISTRIBUTED LEDGER(S)
305
VERIFY INTEGRITY OF TRANSACTIONAL FLOWS
307
TRANSFER CURRENCY TO DESTINATION
309

FIG. 3

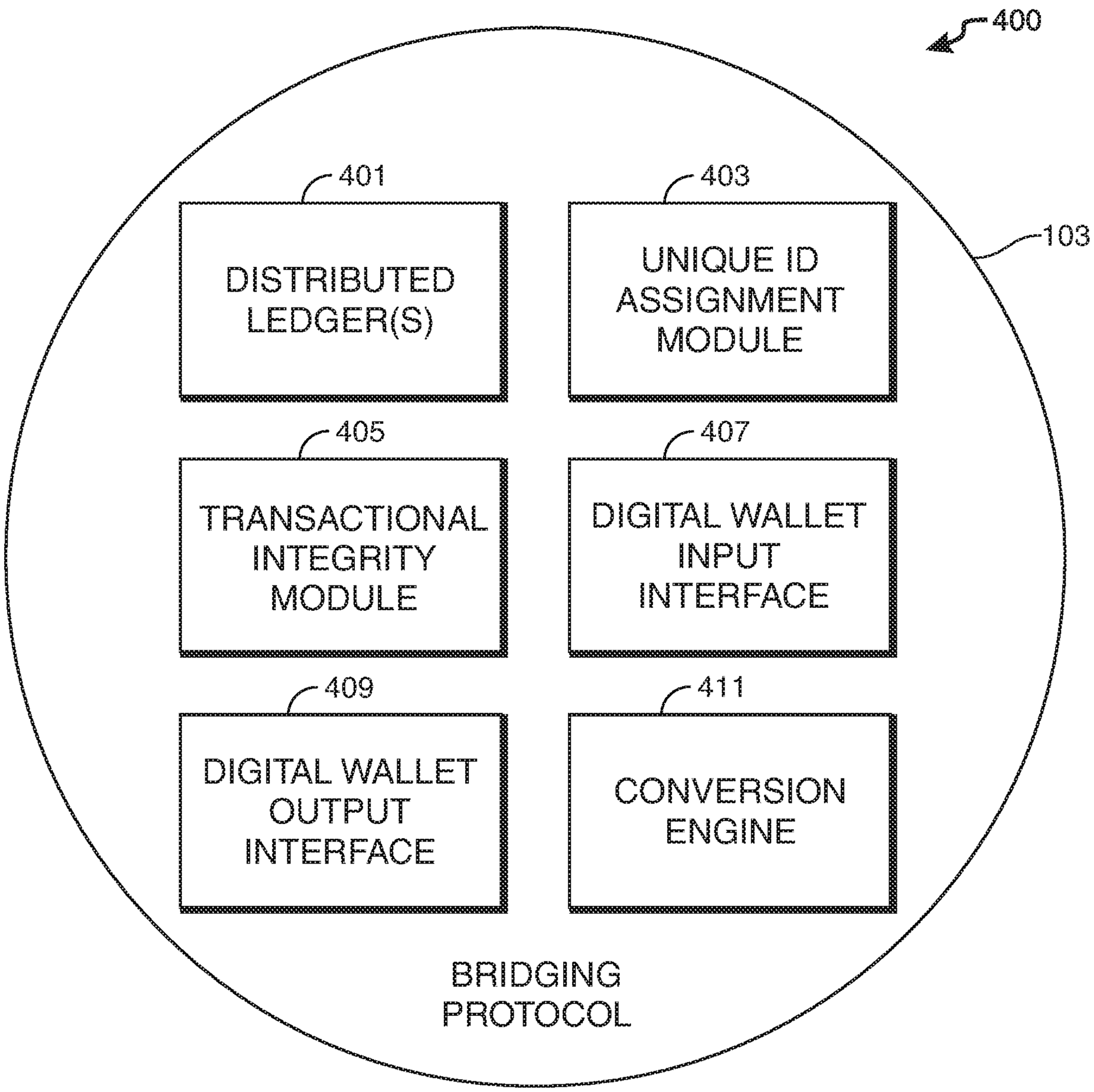

400
103
401
DISTRIBUTED LEDGER(S)
403
UNIQUE ID ASSIGNMENT MODULE
405
TRANSACTIONAL INTEGRITY MODULE
407
DIGITAL WALLET INPUT INTERFACE
409
DIGITAL WALLET OUTPUT INTERFACE
411
CONVERSION ENGINE
BRIDGING PROTOCOL

FIG. 4

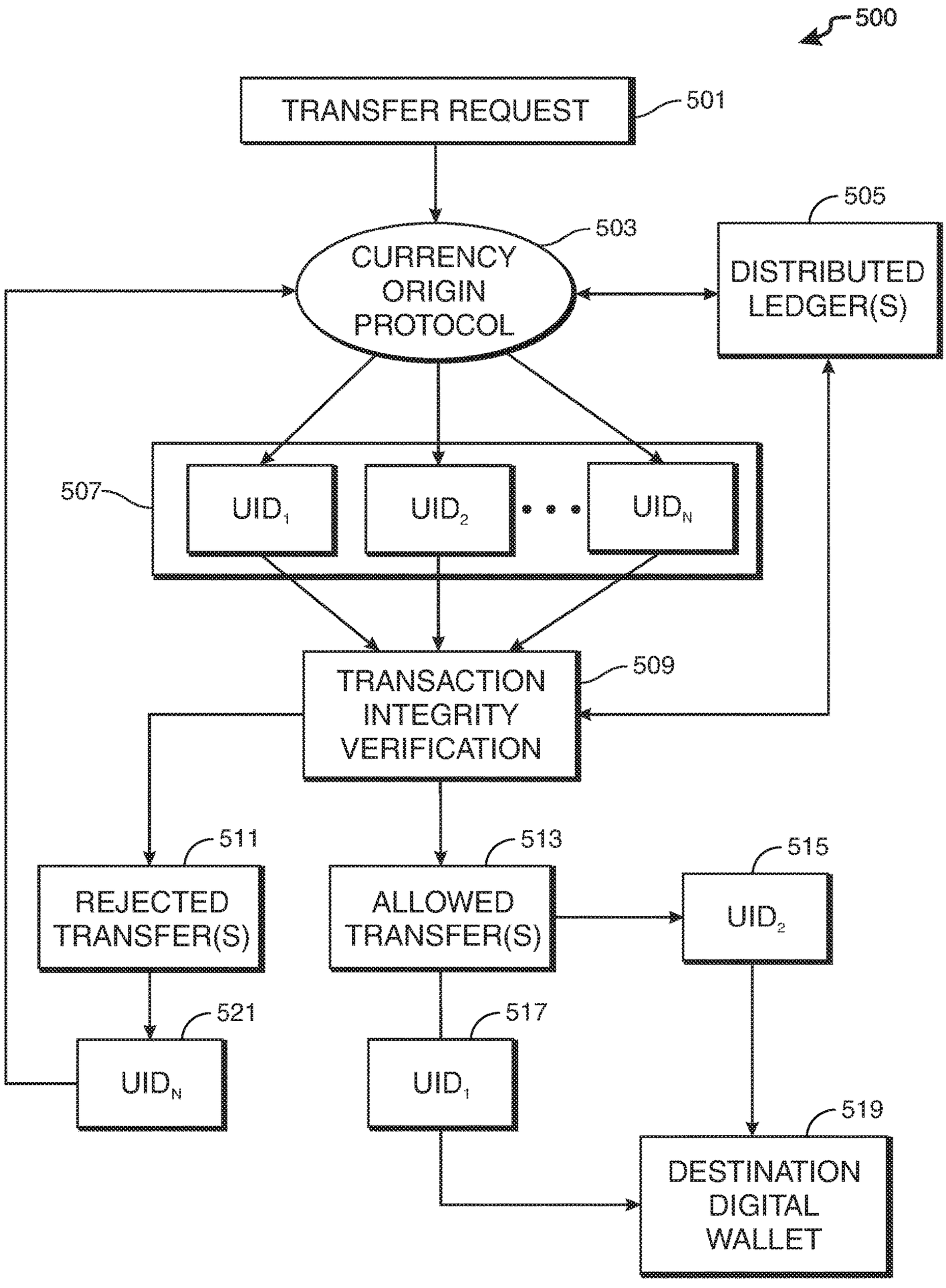

500
TRANSFER REQUEST
501
505
503
CURRENCY ORIGIN PROTOCOL
DISTRIBUTED LEDGER(S)
507
UID1
UID2
UIDN
509
TRANSACTION INTEGRITY VERIFICATION
511
513
515
REJECTED TRANSFER(S)
ALLOWED TRANSFER(S)
UID2
521
517
UIDN
UID1
519
DESTINATION DIGITAL WALLET

FIG. 5

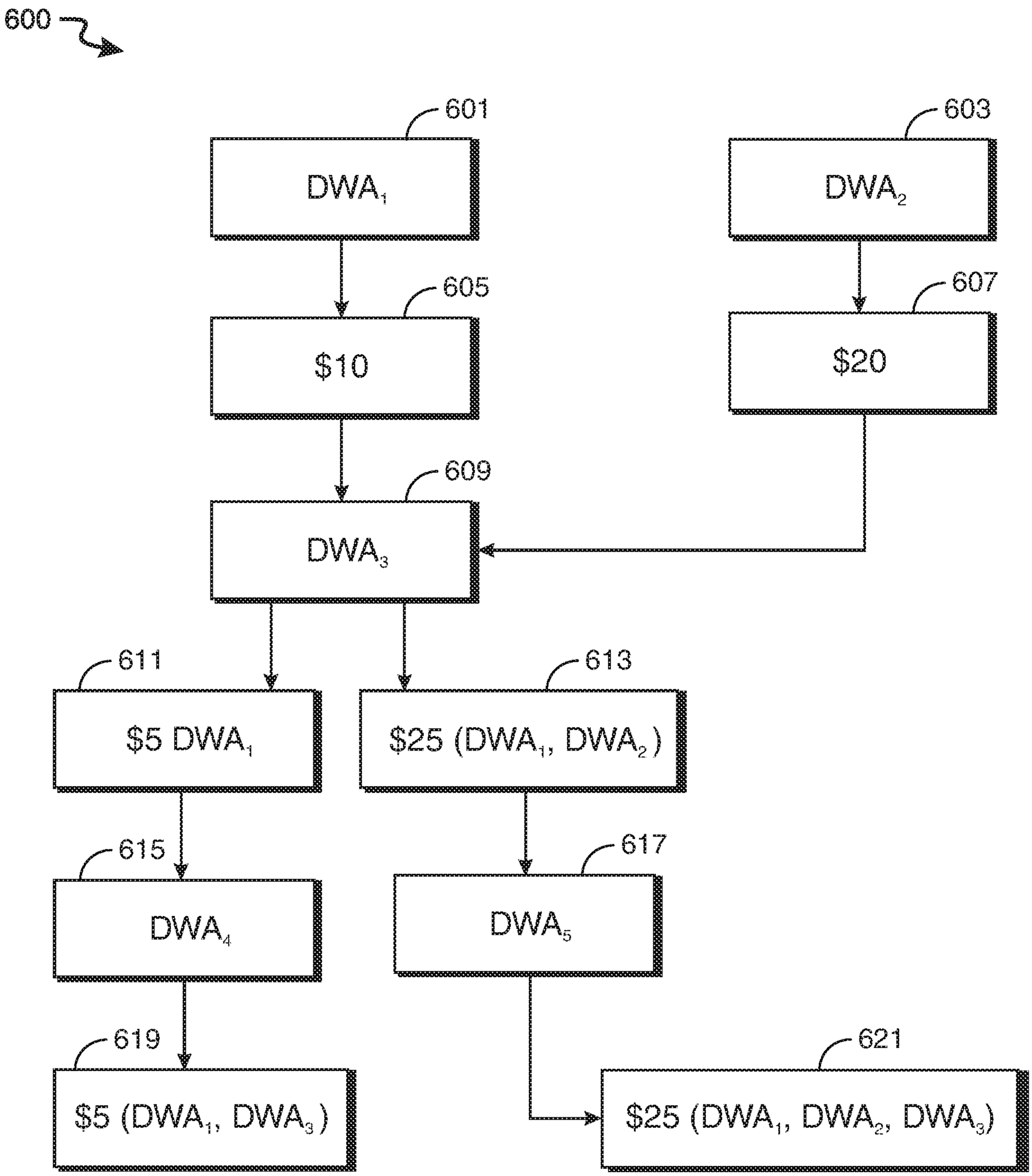

600
601
DWA1
603
DWA2
605
$10
607
$20
609
DWA3
611
$5 DWA1
613
$25 (DWA1, DWA2)
615
DWA4
617
DWA5
619
$5 (DWA1, DWA3)
621
$25 (DWA1, DWA2, DWA3)

FIG. 6

700

701

Record 1: Transfer of $10 by DWA_1 to DWA_3

SourceName(Cust #1)

Receiver(Cust #2)

Amount ($10)

DestinationWalletID(12345)

CurrencyGenesisSerialnumber(2345-hash)

OriginWallet(SDW1) | Origin WalletID(12345)

Genesis date (MM/DD/YY)

Transaction Date (MM/DD/YY)

transaction_ID (xxxxxx)

703

Record 2: Transfer of $20 by DWA_2 to DWA_3

SourceName(Cust #3)

Receiver (Cust #2)

Amount ($20)

DestinationWalletID(12345)

MoneyGenesisSerialnumber(8765-hash)

OriginWallet(SDW2) | Origin WalletID(54321)

Genesis date (MM/DD/YYYY)

transaction Date (MM/DD/YYYY)

transaction ID (yyyyyy)

705

Record 3: Transfer of $5 by DWA_3 to DWA_4

SourceName(Cust #2)

Receiver (Cust #4)

Amount ($5)

DestinationWalletID(67891)

MoneyGenesisSerialnumber(2345-hash)

OriginWallet(SDW1) | Origin WalletID(12345)

FIG. 7A

Genesis date (MM/DD/YYYY)

transaction Date (MM/DD/YYYY)

transaction_ID (aaaaaa)

705

Record 4: Transfer of $25 from DWA_3 to DWA_5

707

Record 4a: Transfer of $5 from DWA_3 to DWA_5

SourceName(Cust #2)

Receiver (Cust #5)

Amount ($5)

DestinationWalletID(55432)

MoneyGenesisSerialnumber(2345-hash)

OriginWallet(SDW1) | Origin WalletID(12345)

Genesis date (MM/DD/YYYY)

Transaction Date (MM/DD/YYYY)

transaction_ID (cccccc)

709

Record 4b: Transfer of $20 from DWA_3 to DWA_5

SourceName(Cust #2)

Receiver (Cust #5)

Amount ($20)

DesitnationWalletID(55432)

MoneyGenesisSerialnumber(8765-hash)

Originwallet(SDW2) | Origin WalletID(54321)

Genesis date (MM/DD/YYYY)

transaction Date (MM/DD/YYYY)

transaction_ID (vvvvvv)

FIG. 7B

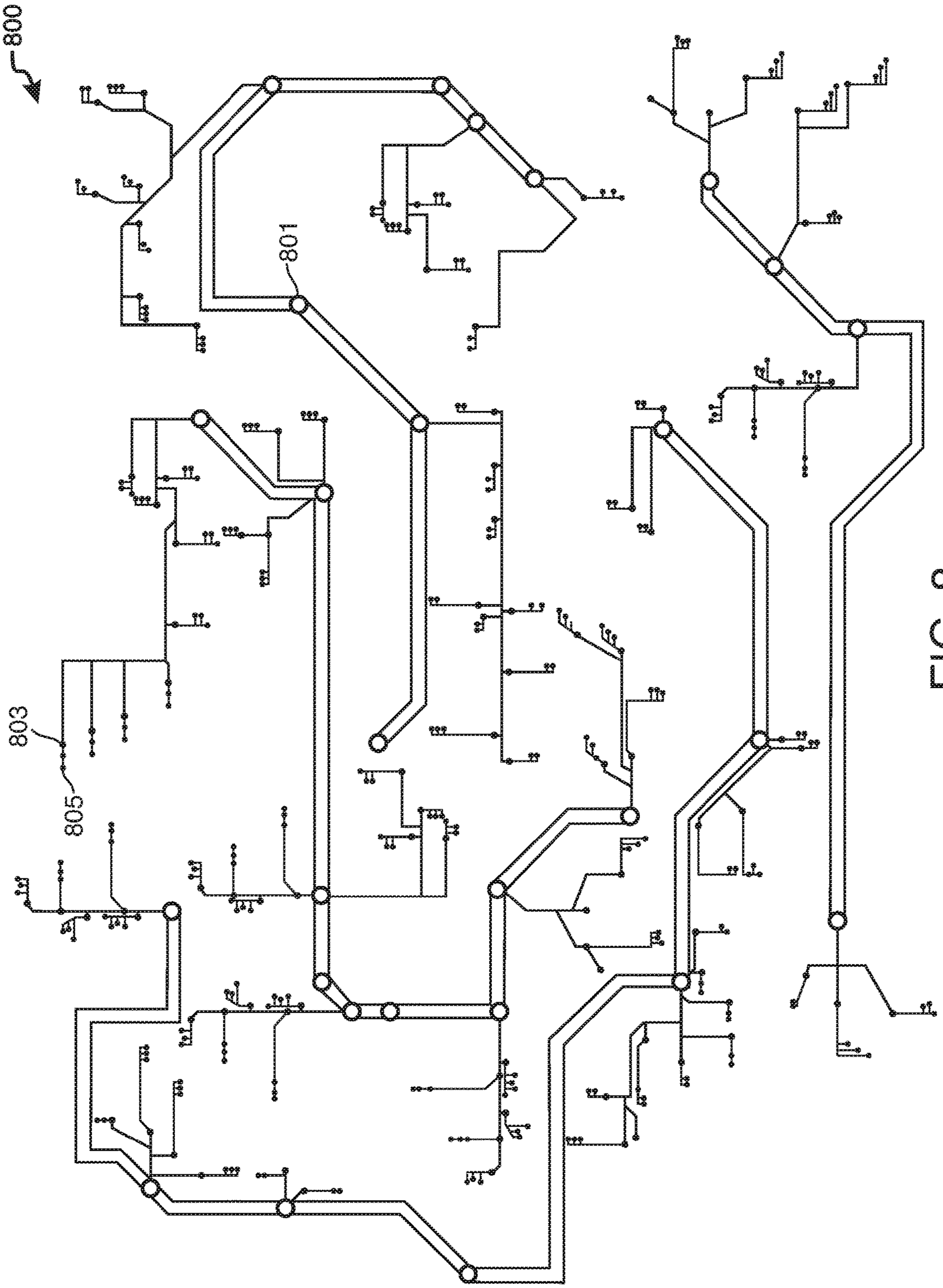


FIG. 8

DIGITAL HOLDING ACCOUNT

FIELD OF TECHNOLOGY

This application describes apparatus and methods for digital payment processing technology.

BACKGROUND

As the world progresses towards a cashless payment society, there has been a rise in the various forms of emerging payment technologies. Such technologies may include digital wallet payment applications.

Many different digital payment applications are now available in the marketplace. However, each digital payment application typically uses its own proprietary technology, communication protocols, data structures and encryption.

There is a need to bridge the gap between these various payment technologies and their respective proprietary ecosystems. Specifically, it would be desirable to provide a hardware device that is configured to seamlessly interact with multiple proprietary payment ecosystems at a merchant POS terminal. Accordingly, it is desirable to provide apparatus and methods for a DIGITAL HOLDING ACCOUNT.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects and advantages of the disclosure will be apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

FIG. **1** shows an illustrative system in accordance with principles of the disclosure;

FIG. **2** shows an illustrative system in accordance with principles of the disclosure;

FIG. **3** shows an illustrative process in accordance with principles of the disclosure;

FIG. **4** shows illustrative system components in accordance with principles of the disclosure;

FIG. **5** shows an illustrative process in accordance with principles of the disclosure;

FIG. **6** shows an illustrative process in accordance with principles of the disclosure;

FIGS. **7**A and **7**B show illustrative information in accordance with principles of the disclosure; and

FIG. **8** shows an illustrative mapping in accordance with principles of the disclosure.

DETAILED DESCRIPTION

As the world progresses towards a cashless payment society, there has been a rise in the various forms of emerging payment technologies. Such technologies may include digital wallet payment systems. There is a need for a bridging protocol and conversion engine that would connect gaps between these various emerging payment technologies and their respective proprietary ecosystems. There is also a need for a digital holding account that provides a protective layer to fund transfers between cashless ecosystems. The digital holding account may hold and monitor currency processed by the conversion engine. Such currency would not be transferred directly into checking account. The digital holding account may be subject to rigorous validations to scrutinize the source and destination of transferred

currency. Validation may include checking distributed ledger transaction records of prior transfers of the received currency.

Apparatus for bridging between multiple digital wallet systems is provided. Apparatus may include a bridging protocol that orchestrates communication between otherwise incompatible digital wallet systems. The bridging protocol may include machine executable instructions running on a computing system. The executable instructions may be self-executing and trigger actions at specified times and/or based on reference to the occurrence or non-occurrence of a target action or event. Some or all of the computer executable instructions may be embodied in hardware or firmware components of a computing system.

The incompatible systems may be digital payment systems. Digital payment systems are typically configured to communicate between users of such systems. The users may run software and/or hardware (collectively, client equipment) that is compatible with the digital payment system.

Typically, a user operating client equipment compatible with one digital payment system is unable to transfer or receive currency from a user operating client equipment compatible with another digital payment system. Currency may include conventional currencies (e.g., USD, EUR, AUD, GBP, JPY, CAD). Currency may include cryptocurrencies (e.g., Bitcoin, Ethereum, Ripple, Bitcoin Cash, NEM, Litecoin, IOTA, NEO, Dash, Qtum, Monero and/or Dogecoin). A digital payment system may apply proprietary security requirements and formulate proprietary communications that are not understood by other digital payment systems and client equipment associated with those other digital payment systems.

The bridging protocol may receive a request. The request may be initiated by a source digital wallet system. The request may ask a digital wallet system to transfer currency to a destination digital wallet system. The source digital wallet system may operate using a first data or communication format. The first format may be proprietary. The destination digital wallet system may operate using a second data or communication format. The second format may be proprietary. The source digital wallet system may be unable to process information generated by the destination digital wallet system. The destination digital wallet system may be unable to process information generated by the source digital wallet system.

The bridging protocol may locate currency associated with the source digital wallet system. The currency may be identified in the transfer request. The currency may be associated with a digital wallet. A digital wallet may refer to electronic devices and programs used for making payments or purchases digitally, without presenting a physical credit card, debit card, or cash. A digital wallet may include an electronic device (e.g., smartphone) that stores payment information and the computer program (e.g., application) used to make the payment. A digital wallet may also hold other information, such as identity credentials, transportation tickets, event tickets, loyalty or gift credentials.

The bridging protocol may locate the currency via communication with a financial institution holding funds associated with the source digital wallet system. The bridging protocol may locate the currency via communication with a distributed ledger that maintains a record of funds associated with the source digital wallet system.

The bridging protocol may assign a unique identifier to the currency of the transfer request. The unique identifier may be an identifier that will be associated with the amount of currency as the currency moves from wallet to wallet

within one or more digital payment systems. The bridging protocol may record the unique identifier in a distributed ledger. The bridging protocol may record attributes associated with a digital wallet or digital wallet system in the distributed ledger. Illustrative attributes are listed below in Table 1:

Table 1: Illustrative Attributes

- Source Digital Wallet System
- Recipient Digital Wallet System
- Name of sender
- Name of recipient
- Amount
- Currency Origin Digital Wallet System
- Currency Origin Wallet ID
- Source Wallet ID
- Destination Wallet ID
- Unique Identifier
- Unique Identifier Assignment Date
- Current Transaction Date
- Current Transaction ID
- Source of Currency (e.g., Checking account, Cash deposit, paycheck, gift)
- Institution holding source currency
- Destination Institution
- Identity of banking institution holding currency associated with a digital wallet (e.g., routing number)
- Account Number at banking institution holding currency associated with a digital wallet

The bridging protocol may validate a transactional integrity of the currency identified in the transfer request. Validating the transactional integrity may include generating a map of the flow of currency assigned the unique identifier. The map may include a flow of the currency from one digital payment system to another digital payment system. The map may include a flow between users of a single digital payment system.

Validating the transactional integrity may include determining an origin of the currency. The origin may be a record of the currency previously created by the bridging protocol. Validating the transactional integrity may include analysis of the map. The analysis may include determining whether the map includes repeating transfer patterns. Repeating transfer patterns may include currency transfers having common attributes.

For example, the mapping may show that the currency was included in multiple transfers that each involved a threshold number of common senders and recipients. Each transfer may utilize a different digital wallet system. Each transfer may be associated with currency earmarked for a particular use. Each transfer may be associated with a particular amount of currency. Each transfer may be associated with a particular geographic location.

The bridging protocol may be configured to validate the transactional integrity by identifying repeating transfer patterns in the mapping.

When the transactional integrity is above a threshold level (e.g., less than a threshold number of repeating transfer patterns), the bridging protocol may disseminate the transactional integrity to each digital payment system that participated in a transfer of the currency assigned the unique identifier. The bridging protocol may inform each digital wallet system for a given transaction is above the threshold level. The transactional integrity may be used to validate a source of currency. The transactional integrity may identify risk factors before accepting funds into a digital payment system. Such risk factors may include unusual or suspicious transfer patterns.

The bridging protocol may utilize a gossip communication bridging protocol to share the transaction integrity with other digital payment systems. A gossip communication bridging protocol may include a procedure or process of computer communication formulated based on the way epidemics spread. Such communication may include peer-to-peer communication without centralized control to ensure that the transactional integrity is received by each of the multiple digital payment systems.

When the transactional integrity is above a threshold level (e.g., less than a threshold number of repeating transfer patterns), the bridging protocol may initiate a transfer of the currency to the destination digital wallet system. The destination wallet system may utilize client equipment that is incompatible with the source digital wallet system. The bridging protocol may formulate data and communications that are compatible with the destination digital wallet system.

The bridging protocol may be configured to receive a transfer request from a first digital wallet system in first data format. The bridging protocol may be configured to transfer the currency to the destination digital wallet system in a second data format.

When the transactional integrity is below the threshold the bridging protocol may be configured to reject the transfer request. The transaction integrity may be below the threshold when the mapping of the currency flow includes a threshold number of repeating transfer patterns. The repeating transfer patterns may include multiple transfers that involve a target source digital wallet system and/or a specific user or device associated with the source digital wallet system. The repeating transfer patterns may include multiple transfers that involve a target destination digital wallet system and/or specific user or device associated with the destination digital wallet system.

The bridging protocol may disseminate a rejection of a transfer request to each digital currency system that transferred currency assigned the unique identifier. The bridging protocol may be configured to block future transactions that include currency having the unique identifier.

The bridging protocol may be further configured to locate a source account corresponding to the source digital wallet system. The source account may be located based on a geographic location associated with a source digital wallet. The source account may be located based on the unique identifier assigned to the currency. The source account may be located based on an identity of the sender of the currency. The sender may be a name or other identifying information assigned to the source digital wallet.

The bridging protocol may locate a destination account. The destination account may correspond to the destination digital wallet. The destination account may be located based on a location associated with the destination digital wallet. The destination account may be located based on the unique identifier assigned to currency. The destination account may be located based on an identity of the recipient of the currency. The destination may be a name or other identifying information assigned to the destination digital wallet.

The bridging protocol may debit the source account and credit the destination account. The credit and the debit may require access to currency transfer networks such as the Federal Reserve Wire Network ("Fedwire"), Clearing House Interbank Payments System ("CHIPS"), Society for Worldwide Interbank Financial Telecommunication ("SWIFT") and other suitable settlement networks known to those of skill in the art.

The bridging protocol may record the credit and debit in one or more distributed ledgers. The bridging protocol may be further configured to record the transactional integrity associated with a transfer in the distributed ledger. A distributed electronic ledger may store records in any suitable format. For example, records may be stored sequentially as they are generated, one after the other in a continuous ledger. Records may be stored in blocks, such as in a blockchain.

The distributed ledger may be a public or unpermissioned distributed ledger. A public distributed ledger does not have restriction on who may participate in the establishing a consensus for adding a new record. For example, records stored in a public distributed ledger may only be added to the ledger when systems that rely on the distributed ledger (e.g., digital payment system or systems responsible for maintaining the source or destination accounts) reach a consensus. The distributed ledger may use any suitable consensus algorithm such as Proof of Work, Proof of Stake or Practical *Byzantine* Fault Tolerance.

The distributed ledger may be a private or permissioned distributed ledger. A private distributed ledger may include restrictions on who may participate in the establishing a consensus for adding a new record.

The distributed ledger may utilize a combination of private and public participation to establish a consensus. For example, the distributed ledger may require a threshold number of private and/or public concurrences before recording a transaction on the distributed ledger. Utilization of private entities may allow for achieving a consensus (or rejection) of a transaction faster than wholly public distributed ledgers.

The distributed ledger may be a blockchain. Records stored in a blockchain are organized in blocks. Each block may include multiple records. The blocks are linked to one another and secured using cryptography.

The bridging protocol may record one or more attributes associated with a currency transfer in a distributed ledger. Illustrative attributes may include a type of currency (e.g., USD, EUR, AUD, GBP, JPY, CAD), an amount of currency, a source digital wallet system and the destination digital wallet system. A distributed ledger may link digital currency transactions based common attributes shared by the transactions. The common attributes may be used to generate a map depicting flow the currency. Common attributes may include the unique identifier assigned to currency. Common attributes may include parties (e.g. source, destination) associated with a digital currency transaction.

The bridging protocol may be configured to move the currency from the source account into a digital holding account. The currency may be moved into the holding account after the bridging protocol receives the request for transferring the currency. The digital holding account may hold the currency until the bridging protocol validates the transactional integrity.

After validating the transactional integrity, the bridging protocol may transfer the currency to a destination digital wallet system. If the transaction integrity is below the threshold, the bridging protocol may transfer the currency back to the source digital wallet system. The bridging protocol may be configured to reject future transactions that include currency transferred back to a source digital wallet system. The bridging protocol may identify such currency based on a unique identifier assigned to the currency. The bridging protocol may be configured to inform the multiple digital currency systems of the rejection. The bridging protocol may inform the multiple digital payment application of the rejection using a gossip communication bridging protocol.

A bridging protocol for bridging between multiple digital currency systems is provided. The bridging protocol may be configured to receive a request initiated by a source digital wallet system. The source digital wallet system may use a first proprietary communication or data format. The source digital wallet system may request a transfer of an amount of currency to a destination digital wallet system. The destination digital wallet system may use a second proprietary communication or data format. The first and second proprietary formats may be incompatible with each other.

The bridging protocol may be configured to validate a transactional integrity of the amount. The bridging protocol may be configured to validate the transactional integrity using a unique identifier assigned to the amount. The unique identifier may have been assigned to the amount by the bridging protocol in connection with a previous transaction.

When the transactional integrity is above a threshold, the bridging protocol may disseminate the transactional integrity to multiple digital currency systems. The transactional integrity may be circulated among the digital currency systems using a gossip-type communication protocol. The bridging protocol may circulate the transactional integrity to each digital currency system that has received currency included in the amount and assigned a common unique identifier.

The bridging protocol may formulate communications with the source digital wallet system in the first format. Using the first format, the bridging protocol may debit an account or digital wallet controlled by the source digital wallet system. Using the first format, the bridging protocol may transfer the amount from an account or digital wallet controlled by the source digital wallet system to a digital holding account. Access to the digital holding account may be controlled by the bridging protocol.

The bridging protocol may formulate a transfer of the amount held in the digital holding account in the second proprietary format used by the destination digital wallet system. The bridging protocol may formulate any communication with the destination digital wallet system in the second proprietary format. For example, using the second format, the bridging protocol may credit an account or digital wallet controlled by the destination digital wallet system. Using the second format, the bridging protocol may effectuate a transfer the amount from an account or digital wallet controlled by the source digital wallet system to the destination digital wallet system. The bridging protocol may effectuate the transfer via a digital holding account. The digital holding account may be controlled by the bridging protocol.

When a transactional integrity of the currency identified in a transfer request is below the threshold, the bridging protocol may be configured to reject the transfer request. In some embodiments, when the transactional integrity is below the threshold, the bridging protocol may quarantine currency identified in a transfer request and held in the digital holding account.

Validation of the transactional integrity may be performed by a smart contract running on a distributed ledger. A smart contract may include machine executable instructions running on a computing system. The executable instructions may be self-executing and trigger actions at specified times and/or based on reference to the occurrence or non-occurrence of a target action or event. Some or all of the computer

executable instructions may be embodied in hardware or firmware components of a computing system.

The bridging protocol and associated smart contracts may be run in cloud computing environments that include virtual software implementations. Such virtual software implementations may be designed to run on a physical hardware supplied externally by a hosting provider, a client, or other platform. The bridging protocol and associated smart contracts may include computer executable instructions for invoking user functionality related to communication, such as email, short message service ("SMS"), and voice input and speech recognition applications.

The bridging protocol and associated smart contracts may utilize computer-executable instructions, such as program modules, executed by a processor on the computing system. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. The bridging protocol and associated smart contracts may be operational with distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices. The bridging protocol and associated smart contracts may rely on a network of remote servers hosted on the Internet to store, manage, and process data (e.g., "cloud computing" and/or "fog computing"). For example, smart contracts may be run on nodes that form a blockchain environment.

The amount included in a transfer request may include currency associated with a first unique identifier. The amount included in the transfer request may include currency associated with a second unique identifier. The unique identifier may allow the currency to be traced back to an originating source. Each transfer request that includes the currency may be associated with the unique identifier. For example, a transaction record associated with each transaction may include the unique identifier. The transaction record may be recorded in a distributed ledger.

The bridging protocol may be configured to execute a first validation routine for a first amount of the currency. The bridging protocol may be configured to execute a second validation routine for the second amount of the currency.

A first amount of the currency may be associated with a first identifier and a first transactional integrity. A second amount of the currency may be associated with a second identifier and a second transactional integrity. The bridging protocol may validate a comprehensive transactional integrity for the transfer request (first and second amounts). The comprehensive transactional integrity may be based on the first validation routine applied to the first amount. The comprehensive transactional integrity may be based on the second validation routine applied to the second amount.

The transactional integrity for the first amount may be above the threshold. The transactional integrity for the second amount may be below the threshold. The transactional integrity for the first amount may be below the threshold. The transactional integrity for the second amount may be above the threshold. The transactional integrity for the first and second amounts may be above the threshold. The transactional integrity for the first and second amounts may be below the threshold.

The bridging protocol may be configured to transfer the first amount to the destination digital wallet system and reject the request to transfer the second amount. For example, the transaction integrity for the first amount may be above the threshold and the transactional integrity for the second amount may be below the threshold.

In some embodiments, when the transactional integrity associated with the first or second amounts is below the threshold, the bridging protocol may be configured to reject the transfer of the first and second amounts. The bridging protocol may be configured to propagate the rejection of a request to each of the multiple digital wallet systems. The bridging protocol may propagate the rejection to each of the multiple digital wallet systems in a proprietary format usable by each digital wallet system.

A transfer request may be a first request to transfer a first amount from a source digital wallet system to a destination digital wallet system. The bridging protocol may be configured to receive a second request. The second request may be initiated by the destination digital wallet system that received the first amount from the source digital wallet system. The destination digital wallet system may request a transfer of a second amount of currency. The second amount of currency may be larger amount than the first amount received from the source digital wallet system.

The bridging protocol may be configured to validate the transactional integrity of the second request. The bridging protocol may classify an amount of currency as being included in the first or second amount using a first-in-first-out ("FIFO") currency management.

For example, User1 may send $10 to Recipient1. A digital wallet of User1 may operate using digital wallet system A. A digital wallet of Recipient1 may operate using digital wallet system B. User2 may send $20 to Recipient1. A digital wallet of User2 may operate using digital wallet system C. The bridging protocol may allow Recipient1 to receive both transfers despite each of User1, User2 and Recipient1 using different digital currency systems. In this case, the bridging protocol may ensure that Recipient1's digital wallet operating on digital wallet system B shows a total balance of $30.

The bridging protocol may assign a first unique identifier to the $10 transferred by User1 to Recipient1. The bridging protocol may assign a second unique identifier to the $20 transferred by User2 to Recipient1.

Recipient1 may then initiate a transfer of a sub-amount of the currency to Recipient2. A digital wallet of Recipient2 may operate using digital wallet system D. Recipient1 may transfer sub-amount $5 to Recipient2 out of the $30 balance. The bridging protocol may use FIFO currency management to determine the unique identifier associated with the transfer from Recipient1 to Recipient2.

For example, using FIFO, the bridging protocol may determine that the $10 Recipient1 received from User1 was "first in" to Recipient1's digital wallet. Therefore, when Recipient1 sends sub-amount $5 to Recipient2, the bridging protocol may assume that the sub-amount $5 is associated with the unique identifier assigned to the transfer originally received from User1.

Continuing with this example, the bridging protocol may register a balance for Recipient2 in digital wallet system D of $5. The bridging protocol may record Recipient2's balance (e.g., in a distributed ledger) as being associated with the same unique identifier assigned to the currency ($10) received by Recipient1 from User1.

Recipient1 may have a balance of $25 in digital wallet system B. Using a FIFO implementation, the bridging protocol may classify Recipient1's balance as including sub-amount $5 from User1 and sub-amount $20 from User2. Recipient1 may now request a transfer of $25 to Recipient3. The bridging protocol may treat the transfer to Recipient3 as

including sub-amount $5 having the unique identifier assigning to currency received from User1 and sub-amount $20 having the unique identifier assigning to currency received from User2.

Methods for managing transfers of currency between multiple digital payment systems are provided. The multiple digital wallet systems may be incompatible with each other. Incompatibility may include a first digital wallet system that cannot receive or transfer funds directly to a second digital wallet system. Communication generated by the first digital wallet system may not be understood by the second digital wallet system. Communications generated by the second digital wallet system may not be understood by the first digital wallet system.

Methods may include transferring a first amount of currency from a source digital wallet system to a first destination digital wallet system. Methods may include assigning a unique identifier to the first amount of currency. The unique identifier may correspond to a source of the first amount.

Methods may include receiving a request to transfer a second amount of currency from the first destination digital wallet system to a second destination digital wallet system. Methods may include validating the transactional integrity of the second amount. Validating may include generating a mapping of movement of the first amount among the multiple digital wallet systems. Using the example provided above, the mapping may include a flow of currency from User1→Recipient1→Recipient2. Using the example provided above, the mapping may include a flow of currency from User2→Recipient1→Recipient3.

Methods may include determining whether the validating yields a transactional integrity that is above or below a threshold level. The threshold level may be determined based on indicators developed when assessing transfers of currency between conventional bank accounts. The threshold level may be determined based on location of the transferee, location of the transferor, attributes of prior transfers associated with the unique identifier assigned to currency included in currency transfer.

Methods may include identifying repeating transfer patterns in the mapping. Repeating transfer patterns may indicate that a particular digital wallet or digital wallet system has participated in a threshold number of transactions involving the same currency. The threshold number of transactions may correspond to a disproportionate number of transactions associated with a target digital wallet or digital wallet system compared to the number of currency transfers processed by the bridging protocol on behalf of other digital wallets or digital wallet systems.

Repeating transfer patterns may indicate that currency is disproportionately flowing into or out of a particular digital wallet or digital wallet system. Based on attributes associated with a digital wallet or digital wallet system, the repeating transfer patterns may indicate that currency is disproportionately flowing into or out of a particular geographic region.

When the mapping includes less than a threshold number of repeating transfer patterns, the transactional integrity register as being above a threshold level. When the transaction integrity is above the threshold level, methods may include transferring the second amount to the second destination digital wallet system. When the threshold integrity is below the threshold level, methods may include imposing a time delay on the transferring of the second amount to the second destination digital wallet system. The time delay may be minutes, hours, days, months or any suitable duration of time.

The time delay may provide additional time to investigate the currency transfer before transferring the currency out of a digital holding account to a destination digital wallet.

Methods may include attempting to conduct additional analysis of the mapping during the time delay. If the additional analysis raises the transactional integrity above the threshold, the bridging protocol may execute the transfer request. If the additional analysis does not raise the transactional integrity above the threshold prior to expiration of the time delay, the transfer request may time-out.

After a transfer request times-out, the transferor may be required to submit a new transfer request. In some embodiments, the bridging protocol may determine that currency is available that would generate a transaction integrity above the threshold level. The bridging protocol may substitute the currency (or amount of the currency) that is needed to complete the transfer request with other currency having a transaction integrity above the threshold level. For example, using FIFO, the bridging protocol attempt to use currency that was provided to the transferor immediately prior the currency associated with the transactional integrity below the threshold level.

The bridging protocol may reject currency associated with a specific unique identifier that is associated with a transactional integrity below the threshold level. When currency is rejected, the bridging protocol may reject any future transfer requests that include the rejected currency.

Methods may include informing each digital payment system of the time delay. Methods may include informing each digital payment system of rejected currency. Method may circulate a message to each digital payment system using a gossip bridging protocol.

A system that secures digital payment transfers is provided. The system may include a digital currency holding account. The system may include an interface layer. The interface layer may be configured to communicate with a source digital wallet application. The source digital wallet application may provide an end user with access to functionality provided by a source digital wallet system. Illustrative functionality may include currency transfers, bill payment or other suitable transactions. A digital wallet application may be installed on the end users mobile device. In some embodiments, the interface layer may interact directly with the source digital wallet system.

The interface layer may be configured to extract a source account from a transfer request generated by the source digital wallet application. The source account may be identified based on an email address, geographic address, phone number, name, social media account, or any other suitable identifier included in the transfer request. The interface layer may be configured to transfer currency from the source account to the digital currency holding account.

The interface layer may be configured to transfer the currency from the digital holding account to a destination account. The destination account may be identified based on an email address, geographic address, phone number, name, social media account, or any other suitable identifier included in the transfer request.

The system may include a security layer. The security layer may be configured to validate a transactional integrity of the currency. When the transactional integrity is successfully validated, the interface layer may initiate a transfer the currency from the digital holding account to the destination account. The destination account may be any suitable account. For example, the destination account may be a demand deposit account or a credit card account.

When the transactional integrity is determined to be invalid, the interface layer may transfer the currency from the digital holding account back to the source account.

The security layer may validate the transactional integrity of the currency by mapping a flow of the currency. The mapping may trace a flow of the currency from a reference point to the source digital wallet application. The security layer may determine whether the mapping includes a threshold number of repeating transfer patterns. Detection of the threshold number of repeating transfer patterns may correspond to an "invalid" transaction integrity. Detection of less than the threshold number of repeating transfer patterns may correspond to a "valid" transaction integrity.

The destination account may be linked to a destination digital wallet system. An end user may access the destination digital wallet system via a destination digital wallet application. The destination digital wallet application may be installed on the end users mobile device.

The interface layer may be configured to communicate with the destination digital wallet application. The interface layer may utilize a proprietary data/communication format when interacting with the destination digital wallet application. In some embodiments, the interface layer may interact directly with the destination digital wallet system. The interface layer may communicate with the destination application or system such that information generated by the interface layer is perceived as coming from the source digital wallet application or system.

The interface layer may be configured to access the source account by interacting with a first computer system operated by a first financial institution. A financial institution may be a bank that controls access to an account. The interface layer may access the digital currency holding account by interacting with a second computer system operated by a second financial institution. The interface layer may access the destination account by interacting with a third computer system operated by a third financial institution.

Each financial institution may employ unique data and/or communication formats. Each financial institution may employ a unique security scheme that requires a specific set of credentials to access an account. The interface layer may be configured to formulate communications compatible with a particular financial institution based on information extracted from a currency request.

The security layer may be configured to record each currency transfer to or from the digital currency holding account. Each transfer may be recorded in a distributed ledger. A mapping of currency flow may be generated relative to a reference transfer recorded in the distributed ledger. The reference transfer may correspond to a transfer recorded in the distributed ledger. The reference transfer may correspond to the earliest transfer associated with the currency identified in a transfer request and recoded in the distributed ledger. The reference transfer may be a transfer recorded in the distributed ledger and associated with a target location.

A reference transfer may be identified based on any suitable attribute included in recorded transaction record. For example, a reference transfer may correspond to the earliest transfer associated with the currency identified in a transfer request and recoded in the distributed ledger. Other suitable attributes may include a specific mobile device, end user, financial institution, digital wallet system or time. Suitable attributes may include attributes listed above in Table 1. A

A computer system for bridging multiple digital currency applications is provided. The system may include computer executable instructions. The system may include a processor and other hardware for executing the instructions. The instructions, when executed by the system, may receive a request initiated by a source digital wallet application.

The request may be a currency transfer request to transfer an amount of currency to a destination digital wallet application or system. The system may transfer the amount from a source account linked to the source digital wallet application to a digital holding account.

The system may validate a transactional integrity of the amount. Validating of the transactional integrity may be performed by a smart contract running on a distributed ledger. When the transactional integrity is above a threshold level, the system may initiate a currency transfer of the amount from the digital currency holding account to the destination digital wallet application. The system may be configured to formulate the currency transfer request such that the destination digital wallet application processes the incoming currency as originating from the source digital wallet application. The system may formulate the transfer currency in a data/communication format that is compatible with the destination digital wallet system.

In some embodiments, the system may initiate a transfer of the amount from the digital holding account directly to a destination account associated with the destination digital wallet application.

When the transactional integrity is below the threshold level, the system may transfer the currency from the digital holding account back to the source account. A transactional integrity below the threshold may indicate that the currency identified in the transfer request is associated with unusual or suspicious transfer patterns.

An amount of currency identified in a currency transfer request may include a first sub-amount and a second sub-amount. The computer executable instructions may be configured to run a first validation routine to determine the transaction integrity for the first sub-amount. The computer executable instructions may be configured to run a second validation routine to determine the transactional integrity for the second sub-amount.

The transactional integrity for the first sub-amount may be above the threshold level. The transactional integrity for the second sub-amount may be below the threshold level. The computer executable instructions may be configured to transfer the first sub-amount from the digital holding account to the destination account. The system may reject the requested transfer of the second sub-amount. The system may reject the transfer of the second sub-amount by transferring the second sub-amount from the digital holding account back to the source account. When the transactional integrity for the first sub-amount is above the threshold level and the transactional integrity for the second sub-amount is below the threshold level, the system may be configured to reject a transfer of both sub-amounts.

The system may be configured to validate the transactional integrity by mapping a flow of the amount using a unique identifier assigned by the computer system. The unique identifier may identify an originating source of the amount. The system may identify repeating transfer patterns in the mapping. The repeating transfer patterns may include a threshold number of transfers of currency between the source account and the destination account via the digital holding account. The system may map the flow using any suitable approach for currency management such as first-in-first-out ("FIFO") or last-in-first-out ("LIFO") currency management.

The system may be configured to apply a first security scheme to currency transfers from the source account to the digital holding account. The first security scheme may require credentials from an end user of the source digital wallet system. The system may apply a second security scheme to transfers from the digital holding account to the destination account. The second security scheme may require credentials from an end user of the destination digital wallet system. In some embodiments, the first and second security schemes may require credentials from one or more financial institutions that control the source and/or destination accounts. In some embodiments, the first and second security schemes may require credentials from a financial institution that controls the digital holding account.

Methods for transferring currency between multiple, siloed digital payment systems are provided. Each of the digital payment systems may use a proprietary data/communication format to communicate with a digital wallet application of each system. Each of the digital payment systems may use a proprietary data/communication format to communicate with one or more financial institutions that control bank accounts of the system's end users. There is a need to bridge the gap between these various payment technologies and their respective proprietary ecosystems.

Methods may include transferring currency associated with a source digital payment system to a digital holding account. Methods may include evaluating a transactional integrity of the currency transferred into the digital holding account. The transactional integrity may be evaluated before transferring the currency out of the digital holding account.

Evaluating the transactional integrity may include mapping a flow of the currency among two or more digital payment systems. The flow may trace movement of the currency from one end user to another. The flow may trace movement of the currency from one digital wallet system to another. The flow may trace movement of the currency from one financial institution to another. When the mapping includes less than a threshold number of repeating transfer patterns, methods may include transferring the currency from the digital holding account to a destination digital payment system; and

When the mapping includes a threshold number of repeating patterns, methods may include holding the currency in the digital holding account. If the repeating patterns indicate suspicious activity, the currency may be quarantined in the digital holding account. Methods may include informing each of the digital payment systems of the transaction integrity of currency identified in a transfer request. Methods may include using a gossip protocol to inform each digital wallet system.

Apparatus and methods in accordance with this disclosure will now be described in connection with the figures, which form a part hereof. The figures show illustrative features of apparatus and method steps in accordance with the principles of this disclosure. It is to be understood that other embodiments may be utilized, and that structural, functional and procedural modifications may be made without departing from the scope and spirit of the present disclosure.

The steps of methods may be performed in an order other than the order shown and/or described herein. Method embodiments may omit steps shown and/or described in connection with illustrative methods. Method embodiments may include steps that are neither shown nor described in connection with illustrative methods. Illustrative method steps may be combined. For example, an illustrative method may include steps shown in connection with any other illustrative method.

Apparatus may omit features shown and/or described in connection with illustrative apparatus. Apparatus embodiments may include features that are neither shown nor described in connection with illustrative apparatus. Features of illustrative apparatus may be combined. For example, an illustrative apparatus embodiment may include features shown or described in connection with another illustrative apparatus/method embodiment.

FIG. **1** shows illustrative system **100**. System **100** includes digital wallet systems **101**. Digital wallet systems **101** may each be incompatible with each other. For example, digital payment wallet system$_1$ may be unable to transfer currency to digital wallet system$_2$. Digital wallet system$_2$ may be unable to receive currency from digital wallet system$_a$.

System **100** includes bridging protocol **103**. Bridging protocol **103** may receive transfer requests generated by one or more of digital wallet systems **101**. The transfer requests may be received from a digital wallet application that interfaces with a particular digital wallet system. A digital wallet application may be run on a mobile device of an end user the particular digital wallet system.

In response to receiving a transfer request from digital wallet systems **101**, bridging protocol **103** may utilize conversion engine **105**. Conversion engine **105** may convert a transfer request into a format that may be processed by bridging protocol **103**. Conversion engine **105** may convert a transfer request received from one of digital wallet systems **101** into a format that may be processed by different one of digital wallet systems **101**. In some embodiments, conversion engine **105** may reside entirely within bridging protocol **103**.

In some embodiments, conversion engine **103** may include a client-side application that runs on an end user's mobile device. Bridging protocol **103** may include a server-side application of conversion engine **105**. The client-side application of conversion engine **105** may intercept a transfer request formulated by a source digital wallet application. The client-side application may convert a transfer request into a format usable by bridging protocol **103**.

Conversion engine **105** may be configured to forward currency to digital holding account **107**. After bridging protocol **103** receives the converted transfer request, a server-side application of conversion engine **105** may generate instructions for transferring currency identified in the transfer request from a source account associated with source digital wallet system to digital holding account **107**. After bridging protocol **103** receives the converted transfer request, a server-side application of conversion engine **105** may generate instructions for transferring currency identified in the transfer request from digital holding account **107** to a destination digital wallet system.

Digital holding account **107** may hold currency received from one or more of digital wallet systems **101**. Digital holding account **107** may hold the currency while a transactional integrity of the currency is evaluated by bridging protocol **103**.

When a transactional integrity associated with currency is above a threshold level, the currency may be accessible by hardware digital wallet **111**. Hardware digital wallet **111** may be controlled by one or more digital wallet applications. The digital wallet applications may be stored on hardware digital wallet **111**. Hardware digital wallet **111** may include near field communication ("NFC") functionality. Hardware digital wallet **111** may receive or initiate transfers of currency via NFC communication.

Hardware digital wallet **111** may communicate with merchant POS terminal ("MPOST") **113**. Hardware digital wallet **111** may use NFC to communicate with MPOST **113**. Hardware digital wallet **111** may provide credentials for accessing currency stored in digital holding account **107** to MPOST **113**. MPOST **113** may be configured to initiate a transaction based on credentials provided by hardware digital wallet **111**. FIG. **1** shows that MPOST **113** may submit the credentials to transaction processing networks **109**.

Transaction processing networks **109** may link acquirers, issuers and other transaction participants that process transactions. For example, transaction processing networks **109** may receive an authorization decision from an issuer and transmit the authorization decision to MPOST **113**. In response to receiving a granted authorization decision, MPOST **113** may release a desired product to the user of hardware digital wallet **111**. In response to receiving a denial authorization decision, MPOST **113** may prompt the user to provide an alternative payment method (e.g., cash or check).

Transaction processing networks **109** (in communication with other transaction participants) may settle transactions between the issuer and the acquirer, digital payment applications or any parties to a transaction. A transaction settlement process may include a transfer of funds between two or more transaction participants. A settlement network may transfer the funds between transaction participants. Illustrative settlement networks may include Fedwire or other suitable settlement networks. The settlement network may include any network linking one or more accounts of transaction participants.

System **100** shows that transaction processing networks **109** may transfer funds into digital holding account **107**. Funds transferred into digital holding account **107** may be assigned a unique identifier by bridging protocol **103**. In some scenarios, funds received by bridging protocol **103** may already be associated with a unique identifier previously assigned by bridging protocol **103**.

FIG. **2** shows illustrative system **200**. System **200** includes source digital wallet applications ("SDWA") **201**. Each of SDWA **201** may be an end-user application for interfacing with at least one of digital wallet systems **101**. A user of SDWA **201** may submit a currency transfer request to one or more of destination digital wallet applications ("DDWA") **203**. Each of DDWA **203** may be end-user application for interfacing with at least one of digital wallet systems **101**.

The currency transfer request submitted by SDWA **201** may be intercepted by conversion engine **105** (shown in FIG. **1**). In response to intercepting a transfer request from SDWA **201**, conversion engine **105** may pass the transfer request to security layer **211**. Security layer **211** may evaluate a transactional integrity of currency associated with the transfer request.

For example, security layer **211** may conduct mapping and pattern detection **213**. The mapping may trace a flow of the currency identified in the transfer request. Mapping and pattern detection **213** may access records stored in distributed ledgers **207**. Distributed ledgers **207** may include records of transactions processed by bridging protocol **103** and its associated components. Distributed ledgers **207** may include ledgers maintained by one or more of digital wallet systems **101**.

Distributed ledgers **207** may include records of transactions associated with banks **209**. Distributed ledgers **207** may include records of transactions associated with digital holding account **205**. Distributed ledgers **207** may include records of transactions corresponding to underlying account activity among banks **209** triggered by a currency transfer.

For example, digital wallet systems **101** may not have direct access to underlying bank accounts. Digital currency systems **101** may submit transfer requests to banks **209** that have access to the underlying end user's accounts (source or destination) identified in a currency transfer request.

Distributed ledgers **207** may include records of transactions processed by MPOST **113** and transaction processing networks **109**. Bridging protocol **103** may identify related records. Bridging protocol **103** may identify related records based on common attributes. For example, a unique identifier assigned to currency stored in a record on distributed ledgers **207** may identify a source name associated with currency. The source name may also correspond to a name on an account controlled by banks **209**.

FIG. **3** shows illustrative process **300**. One or more of the steps of the process illustrated in FIG. **3** may be performed by a "system." The "system" may include one or more of the features of the apparatus shown in FIGS. **1-2** and/or any other suitable device or approach. The "system" may be provided by an entity. The entity may be an individual, an organization or any other suitable entity.

Process **300** begins at step **301**. At step **301** the system receives a currency transfer request. The request may be received from a source digital wallet application (e.g., SDWA **201**) asking to transfer an amount of currency to a destination digital wallet application (e.g., DDWA **203**). At step **303**, the system splits currency based on the number of unique identifiers of the currency associated with the received transfer request.

For example, a source digital wallet application may request that an amount of currency be transferred to a destination digital wallet application. The requested amount of currency may include currency received by the source digital wallet application from multiple other sources. Each amount of currency received from the other sources may be assigned a different unique identifier.

At step **305**, the system maps a flow of each amount of the currency assigned a different unique identifier. The flows may be mapped based on entries in one or more distributed ledgers (e.g., distributed ledgers **207**). At step **307**, the system validates a transactional integrity of the currency using on the mapping. Validating the transactional integrity may include determining an origin of each amount of currency included in the received transfer request. An origin may be determined based on tracking a unique identifier assigned to currency and included in each transaction record generated each time the currency is transferred.

Validating the transactional integrity may include confirming that security of a source digital wallet application/system associated with the origin has not been compromised. Validating the transactional integrity may include determining that security of a destination digital wallet application/system has not been compromised.

At step **309**, when the transactional integrity is above a threshold level, the system transfers currency to destination digital wallet application. The transfer to the destination digital wallet application may include formulating communications that are compatible with the digital wallet system of the destination digital wallet application identified in the transfer request received at step **301**.

FIG. **4** shows system **400**. System **400** shows illustrative sub-components of bridging protocol **103**. System **400** includes distributed ledger(s) **401**. Distributed ledger(s) **401** may be used by bridging protocol **103** to store records of each currency transfer processed by bridging protocol **103**.

Distributed ledger(s) **401** may be used by digital wallet systems **101** to store transactions processed by each of those systems. Bridging protocol **103** may record, for each transfer request received from digital wallet systems **101**, the unique identifier assigned to currency identified in the transfer request.

System **400** includes unique identifier assignment module **403**. Assignment module **403** may determine whether a currency amount identified in transfer request received by bridging protocol **103** has already been assigned a unique identifier. Assignment module **403** may split identified currency into amounts. For example, assignment module **403** may use FIFO to assign a unique identifier to different amounts of currency associated with a transfer request. Any suitable accounting method may be used to assign a unique identifier to currency identified in a transfer request. Other suitable accounting methods may include LIFO currency management.

System **400** includes transactional integrity module **405**. Transactional integrity module **405** may generate maps showing movement of currency through one or more of digital wallet systems **101**. Transactional integrity module **405** may generate maps showing movement of currency flowing between different digital wallet systems **101**.

Transactional integrity module **405** may generate heat maps based on one or more unique identifiers assigned to currency in a transfer request. The heat maps may show digital wallet applications and systems (source or destinations) that have been in involved in transactions that include the currency assigned the unique identifiers associated with currency identified a currency transfer request. The heat maps may show repeating patterns detected in the transactions. The patterns may show that relatively large amounts of the currency have been received by particular source or destination digital wallet systems or applications. Such digital wallet systems and applications may be flagged for suspicious activity.

Heat maps generated by transactional integrity module **405** may be compared to heat maps or other transaction information for an entity or specific end user. Other transaction information may include transaction records generated by back end currency movement **205** (shown in FIG. **2**) or transaction processing network **109** (shown in FIG. **1**). If heat maps generated by transaction integrity module **405** show transaction activity for currency that is disproportionate to the transaction information associated with others data sources, the transactional integrity for the currency may be classified as being below a threshold level.

System **400** includes conversion engine **411**. Conversion engine **411** may include a client side application that resides on an end users mobile device. Conversion engine **411** may include a server-side application that resides within bridging protocol **103**. Conversion engine **411** may include one or more features of conversion engine **105** (shown in FIG. **1**).

System **400** includes digital wallet input interface **407**. Interface **407** may be used to receive transfer requests from SDWA **201** (shown in FIG. **2**). System **400** may include an interface **400** for communicating with each of SDWA **201**. Interface **407** may be generated by conversion engine **411**. Interface **407** may transfer currency from SDWA **201** to digital holding account **107**.

In some embodiments, interface **407** may be generated by a client-side application of conversion engine **411**. Interface **407** may be generated by a server-side application of conversion engine **411**.

System **400** includes digital wallet output interface **409**. Interface **409** may be generated by conversion engine **411**. Interface **409** may be used to initiate transfer requests with DDWA **203** (shown in FIG. **2**). System **400** may include an interface **409** for communicating with each of DDWA **203**. Interface **409** may transfer currency from digital holding account **107** to DDWA **203**.

In some embodiments, interface **409** may be generated by a client-side application of conversion engine **411**. In some embodiments, interface **409** may be generated by a server-side application of conversion engine **411**.

System **400** may include one or more integrated circuits which may be configured to perform any suitable logical operation. System **400** may include I/O circuitry, which may include a transmitter device and a receiver device and may interface with fiber optic cable, coaxial cable, telephone lines, wireless devices, PHY layer hardware, a keypad/display control device or any other suitable encoded media or devices. The I/O circuitry may include a microphone, button and/or touch screen which may accept user provided input. The I/O circuitry may include one or more of a speaker for providing audio output and a video display for providing textual, audiovisual and/or graphical output. The video display may include one or more organic light emitting diodes.

I/O circuitry may include a wireless communication circuit. The wireless circuit may provide Wi-Fi, NFC, Bluetooth, satellite, cellular or any other suitable mode of wireless communication. Wi-Fi may include passive Wi-Fi with lower power consumption than typical Wi-Fi. System **400** may include counter timers, real-time timers, power-on reset generators or any other suitable peripheral devices. System **400** may include a processor, which may compute data structural information, structural parameters of the data, generate currency flow maps or detect patterns in the maps. The processor may include sub-components for controlling operation of system **400** and its associated modules.

System **400** may include machine-readable memory. The memory may store applications such as an operating system, application programs, web browser and a database. Application programs may include computer executable instructions for invoking user functionality related to communication, such as email, short message service ("SMS"), and voice input and speech recognition applications. Application programs may utilize one or more algorithms that control prompts presented at a merchant POS terminal, generate virtual interfaces, process received executable instructions, generate executable instructions, perform power management routines or other suitable tasks.

Components of system **400** may be coupled together by a system bus or other interconnections and may be present on one or more circuit boards. In some embodiments, the components may be integrated into a single chip. The chip may be silicon-based.

FIG. **5** shows illustrative process **500**. One or more of the steps of the process illustrated in FIG. **5** may be performed by a "system." The "system" may include one or more of the features of the apparatus or processes shown in FIGS. **1-4** and/or any other suitable device or approach. The "system" may be provided by an entity. The entity may be an individual, an organization or any other suitable entity.

Process **500** begins at step **501**. At step **501** the system receives a transfer request. At step **503** the transfer request is ingested by bridging protocol **503**. At step **505** bridging protocol communicates with distributed ledgers **505**. Distributed ledgers **505** record prior and current transactions processed by bridging protocol **503**. Transfer request **501** may include currency that already has been assigned a unique identifier by bridging protocol **503**.

Bridging protocol **503** may apply an appropriate accounting method (e.g. FIFO, LIFO) to track unique identifiers **507** associated with currency referenced in transfer request **501**. At step **509**, the system may perform transactional integrity validation **509**. Transactional integrity validation **509** may be performed for each of unique identifiers **507** associated with transfer request **501**. Transactional integrity validation **509** may include generating a map of currency flow for each of the unique identifiers **507**. Transactional integrity validation **509** may include analysis of the currency flow maps.

Analysis of the currency flow maps may identify unusual, repeating patterns or other anomalous activity associated with unique identifiers **507**. At step **511**, the system rejects the transfer of currency associated with the movement of currency corresponding to unique identifiers **521**. Currency assigned unique identifiers **521** may have a transactional integrity below a threshold level. For example, analysis of the currency flow maps for unique identifiers **521** may show anomalous or suspicion currency flow patterns.

At step **513**, the system allows the transfer of currency associated with unique identifiers **517** and **515** to destination digital wallet **519**. Currency assigned unique identifiers **517** and **515** may each have a transactional integrity above a threshold level. For example, analysis of the currency flow maps for unique identifiers **517** and **515** may show random flow patterns without a threshold number of repeating patterns.

FIG. **6** shows illustrative currency movement **600**. A bridging protocol such as bridging protocols **103** and **503**, may implement currency movement **600**. Movement **600** shows that destination digital wallet$_1$ ("DDWA$_2$") **601** initiates a transfer of $10 (item **605**) to DDWA$_3$ (item **609**). The $10 (item **605**) may be assigned a first unique identifier. Movement **600** also shows that at step **603**, DDWA$_2$ initiates a transfer of $20 (item **607**) to DDWA$_3$. The $20 (item **607**) may be assigned a second unique identifier.

At step **609**, after transfers **605** and **607**, DDWA$_3$ is associated with a total balance of $30. The total of 30 may be associated with two unique identifiers. At step **611**, DDWA$_3$ requests a transfer of $5 to DDWA$_4$ (item **615**). Step **611** also shows that the $5 selected for transfer to DDWA$_4$ is currency DDWA$_3$ received from DDWA$_2$. The $5 selected for transfer to DDWA$_4$ may be recorded as being associated with the first unique identifier. At step **613**, DDWA$_3$ requests a transfer of $25 to DDWA$_5$ (item **617**). Step **613** also shows that the $25 selected for transfer to DDWA$_4$ is currency DDWA$_3$ received from DDWA$_1$ and DDWA$_2$. The $25 selected for transfer to DDWA$_4$ may be associated with the first and second unique identifiers.

Step **621** shows that after DDWA$_5$ receives the $25 from DDWA$_3$, the $25 is associated with unique identifiers that trace the origin of the currency back to DDWA$_1$, DDWA$_2$ and DDWA$_3$. Step **619** shows that after DDWA$_4$ receives the $5 from DDWA$_3$, the $5 is associated with unique identifiers that trace the origin of the currency back to DDWA$_1$ via DDWA$_3$.

FIGS. **7**A and **7**B show illustrative transaction records that may be generated by currency movement **600** shown in FIG. **6**. The transaction records may be stored in a distributed leger such as distributed ledgers **207**, **401** or **505**. Record **701** includes attributes evidencing the transfer of $10 from DDWA$_1$ to DDWA$_3$. Record **701** shows that the $10 transferred from DDWA$_1$ to DDWA$_3$ is associated with unique identifier ("MoneyGenesisSerialnumber") (2345-hash).

Record **703** includes attributes evidencing the transfer of $20 from DDWA$_2$ to DDWA$_3$. Record **703** shows that the $20 transferred from DDWA$_2$ to DDWA$_3$ is associated with the unique identifier (8765-hash).

Record **705** includes attributes evidencing the transfer of $5 from DDWA$_3$ to DDWA$_4$. Record **705** shows that the $5 transferred from DDWA$_3$ to DDWA$_4$ is associated with the unique identifier (2345-hash), the same unique identifier included in record **701**.

Records **707** and **709** include attributes evidencing the transfer of $25 from DDWA$_3$ to DDWA$_5$. Record **707** shows that $5 transferred from DDWA$_3$ to DDWA$_5$ is associated with the unique identifier (2345-hash). Record **709** shows that $20 transferred from DDWA$_3$ to DDWA$_5$ is associated with the unique identifier (8765-hash).

FIG. **8** shows illustrative mapping **800** of currency flow. Mapping **800** includes large nodes **801**, medium nodes **803** and small nodes **805**. Large nodes **801** may represent digital wallet end users that are associated with a relatively larger number of currency transfers compared to end users represented by nodes **803** or **805**. Large nodes **801** may represent digital wallet end users that are associated with a relatively higher valued currency transfers compared to end users represented by nodes **803** or **805**.

In some embodiments, end users corresponding to nodes **805** may be flagged as being associated with a threshold level of repeating currency transfer patterns or other anomalous activity.

Medium nodes **803** may represent digital wallet end users that are associated with a relatively larger number of currency transfers compared to end users represented by nodes **805**. Medium nodes **803** may represent digital wallet end users that are associated with a relatively higher valued currency transfers compared to end users represented by nodes **805**.

All the currency transfers captured in mapping **800** may include currency that is transferred from a source digital wallet system to a destination digital wallet system via a digital holding account.

Thus, apparatus and methods for a DIGITAL HOLDING ACCOUNT are provided. Persons skilled in the art will appreciate that the present disclosure can be practiced by other than the described embodiments, which are presented for purposes of illustration rather than of limitation. The present disclosure is limited only by the claims that follow.

What is claimed is:

1. A computer system for bridging incompatible and proprietary security protocols of multiple digital wallet applications, the system comprising self-executing computer executable instructions, that when executed by the system:

receive a request initiated by a source digital wallet application using a first security scheme and a first communication protocol to transfer an amount of currency to a destination digital wallet application, wherein the destination digital wallet application uses a second security scheme and communication protocol that are incompatible with the source digital wallet application and the amount comprises a first sub-amount and a second sub-amount of the currency;

orchestrate proprietary security requirements of the multiple digital wallet applications by using a bridging protocol to:

transfer the amount from a source account linked to the source digital wallet application to a digital holding account using the first security scheme and the first communication protocol;

validate a comprehensive transactional integrity of the amount by:

generating a first map of a first flow of the first sub-amount between the source and destination digital wallet applications; and

detecting repeating transfer patterns associated with the first sub-amount that include a target number of common senders and recipients;

generating a second map of a second flow of the second sub-amount between the source and destination digital wallet applications; and

detecting repeating transfer patterns associated with the second sub-amount that include the target number of common senders and recipients;

when less than a threshold number of repeating transfer patterns are associated with each of the first and second sub-amounts:

register that the comprehensive transactional integrity for the amount is above a threshold level;

apply a second security scheme to the amount; and

transfer the amount using a second communication protocol from the digital currency holding account to the destination digital wallet application such that the destination digital wallet application processes the incoming currency as originating from the source digital wallet application in accordance with the second security scheme and second communication protocol; and

when the bridging protocol detects more than a threshold number of repeating transfer patterns for the second sub-amount:

register that the transactional integrity for the second sub-amount is below the threshold level;

transfer the second sub-amount from the digital holding account back to the source account using the first security scheme and the first communication protocol;

block future transactions of the second sub-amount; and

transfer the first sub-amount from the digital holding account to the destination digital wallet application using the second security scheme and the second communication protocol.

2. The computer system of claim **1**, wherein validating the transactional integrity is performed by a smart contract running on a distributed ledger.

3. The computer system of claim **1** the bridging protocol validates the transactional integrity by:

mapping the flow of the first and second sub-amounts using a unique identifier assigned to an originating source of the first and second sub-amounts by the first security scheme.

4. The computer system of claim **1** wherein the repeating transfer patterns comprise a threshold number of transfers between the source account and the destination digital wallet application via the digital holding account.

5. The computer system of claim **3**, the wherein bridging protocol maps the flow using first-in-first-out ("FIFO") currency management.

6. The computer system of claim **1**, wherein: the first security scheme requires a first set of credentials to transfer the amount from the source account to the digital holding account; and

the second security scheme requires a second set of credentials to transfer the amount from the digital holding account to the destination digital wallet application.

7. A system that secures digital currency transfers between incompatible and proprietary security protocols of multiple digital payment systems, the system comprising:

a digital currency holding account;

an interface layer that orchestrates proprietary communication requirements of the multiple digital wallet applications by:

communicating with a source digital wallet application using a first security scheme and a first communication protocol;

extracting a source account from a transfer request generated by the source digital wallet application; and

transferring an amount of currency from the source account to the digital currency holding account using the first security scheme and the first communication protocol, wherein the amount comprises a first sub-amount and a second sub-amount;

a security layer that orchestrates proprietary security requirements of the multiple digital wallet applications by:

validating a comprehensive transactional integrity of the amount by:

generating a first map of a first flow of the first sub-amount from a first reference point to the source account;

generating a second map of a second flow of the second sub-amount from a second reference point to the source account; and

detecting one or more repeating transfer patterns within the first and second flows that include a target number of common senders and recipients;

when the security layer detects less than a threshold number of repeating transfer patterns:

registering the comprehensive transactional integrity as successfully validated; and

utilizing the interface layer to transfer the amount from the digital holding account to a destination account using a second security scheme and a second communication protocol; and

when the security layer detects more than a threshold number of repeating transfer patterns:

registering the comprehensive transactional integrity as invalid;

blocking future digital currency transfers from the source account; and

utilizing the interface layer to transfer the amount from the digital holding account to the source account using the first security scheme and the first communication protocol.

8. The system of claim **7**, wherein:

the destination account is linked to a destination digital wallet application; and

the interface layer is configured to communicate with the destination digital wallet application such that, to the destination digital wallet application, information generated by the interface layer is received from the source digital wallet application.

9. The system of claim **7** wherein the destination account is a demand deposit account.

10. The system of claim **7** wherein the destination account is a credit card account.

11. The system of claim **7**, wherein the interface layer is configured to:

access the source account by interacting with a first computer system operated by a first financial institution;

access the digital currency holding account by interacting with a second computer system operated by a second financial institution; and

access the destination account by interacting with a third computer system operated by a third financial institution.

12. The system of claim **7** wherein the security layer is configured to:

record each transfer to or from the digital currency holding account in a distributed ledger; and

the first and second reference points correspond to reference transfers recorded in the distributed ledger.

13. The system of claim **12**, wherein each of the reference transfers corresponds to an earliest transfer of the first or second sub-amounts recorded in the distributed ledger.

14. The system of claim **12**, wherein the reference transfer are both associated with a target location.

15. A method for transferring currency between multiple, incompatible digital payment systems, each of the digital payment systems utilizing a proprietary security protocol, the method comprising:

transferring currency associated with a source digital payment system to a digital holding account using a first security scheme and a first communication protocol;

orchestrate proprietary security requirements of the multiple digital wallet applications by applying a bridging protocol that evaluates a transactional integrity of the currency by:

mapping a first flow the currency between the incompatible digital payment systems via the digital holding account;

mapping a second flow of the currency among users of the source digital payment system;

detecting a first repeating transfer pattern in the first flow that is associated with a geographic location; and

detecting a second repeating transfer pattern in the second flow that includes a target number of common senders and recipients;

when the first and second mappings include less than a threshold number of first and second repeating transfer patterns:

generating computer executable instructions that transfer the currency to a destination digital payment system using a second security scheme and second communication protocol that are incompatible with the source digital payment system; and

executing the computer executable instructions, thereby transferring the currency from the digital holding account to the destination digital payment system; and

when the mapping includes the threshold number of repeating patterns;

holding the currency in the digital holding account; and

blocking future digital currency transfers of the currency.

16. The method of claim **15** further comprising, informing each of the multiple, siloed digital payment systems of the transactional integrity using a gossip protocol.

* * * * *